Edinburgh Napier
UNIVERSITY

UIGG(18/19)12

EDINBURGH NAPIER UNIVERSITY
RISK & RESILIENCE COMMITTEE

UNIVERSITY INFORMATION GOVERNANCE GROUP

Minutes of the meeting held on Tuesday 19 February 2019
at 2.00pm in Room 5.B.16, Sighthill Campus

Present
D Watt (Information Governance Manager)[Convenor]; R Burns (International Marketing Manager); E Clark (Governance Adviser (Freedom of Information)); B Kieliszek (Information & Operations Manager); N Kivlichan (Head of Market & Student Intelligence); B Merchant (IT Business Change Consultant); D Munro (Communications Manager); A Richmond (Governance Adviser (Records Management)); C Sutherland (Systems Officer); G Thomson (Executive Assistant)
Apologies
P Barron (Professor of Hospitality & Tourism Management); R Bews (Appeals, Complaints & Conduct Manager); D Cloy (University Secretary); L Conlan (Head of HR Services); O Dellal (School Operations Officer); J Dickson (School Support Manager); S Duncan (Head of Campus Services); G Hamilton (Information Security Manager); L McElhone (Head of Student Administration); J Martin (Systems Officer); A Ramsay (Senior HR Adviser); S Simeone (School Operations Officer); L Smith (Operations Support Manager); D Spiers (Lecturer); N Turner (Head of Research and Innovation Office)
In Attendance
M Mackay (Administrative Assistant)[Clerk]
Welcome, Introductions and Apologies
The Information Governance Manager welcomed members to the meeting, extending a particular welcome to new member B Kieliszek. Members who had demitted since the last meeting were thanked for their contributions. The apologies were **noted**.

01	Minutes of the Meeting held on 28 March 2018	UIGG(17/18)12

Members **approved** the minutes of the meeting on 28th March 2018 as an accurate record.

02	UIGG Remit and Constitution	UIGG(18/19)01

Members discussed the potential to expand the remit of UIGG to cover Information Security. It was suggested that extending the remit would offer an opportunity to have a forum to report on information security compliance, security incidents and challenges, and to expand a sense of ownership of information security across the University. Members **approved** the extension of the remit of UIGG. The revised remit would be presented at the next meeting.

03	UIGG Membership	UIGG(18/19)02

Members **noted** the current membership of UIGG, and discussed potential additions to increase representation on the group from across the University. It was suggested that additional members could be sought from Student Recruitment and Admissions, Research and Innovation, Information Services and from the Information Governance Champions. Members were requested to pass any suggestions on to the Convenor.

04	Matters Arising from the Minutes

The IGM informed members that work was progressing well on including Data Sharing Agreements for new contracts across the University. However, potential problems existed with bringing in Data Sharing Agreements for contracts which were already in place. Members were requested to ensure that such agreements were in place where required.

05	Freedom of Information and Records Management a) Report to September 2018 b) Report to January 2019	UIGG(18/19)03 Verbal Report

The Governance Adviser (Freedom of Information) spoke to the paper and highlighted:

- The number of FoI requests received had increased over the reporting period for the previous year. The majority of requests had come from the media, with frequent topics for requests including sexual assault / harassment, misconduct and mental health issues.

- All but six requests had been responded to within 20 days; however, requests had to be chased up with other departments on 60 occasions. There were 19 occasions when no information was provided, with the most common exemption used being Section 38 (personal information).

- Benchmarks against the performance of other Universities placed ENU within the top 50%

- The University's appeal, regarding a request on staff survey comments, with the Scottish Information Commissioner had concluded in ENU's favour. It was raised that future surveys would require careful wording for their privacy statements to ensure confidentiality.

The Communications Manager raised the issue that an increase in requests for information from journalists were being received on Fridays for publication on Sunday, under the threat of citing a refusal to comment. The IGM suggested that the issue could be raised with the Scottish Higher Education Information Practitioners (SHEIP), and the CM suggested that a similar group to co-ordinate HE press staff could also be useful.

06	Data Protection and Records Management Report to January 2019	UIGG(18/19)04

The information Governance Manager spoke to the paper and highlighted:

- Two data breaches had been reported to the Information Commissioner – one involving a third party website, the other a large number of emails. The University's

response had been deemed appropriate in both cases by the Information Commissioner, and no further action was required.

- Twenty-three non-reportable breaches had also occurred, the IGM noted that the incidents had probably happened in similar numbers previously, but staff were now more likely to inform Governance Services.

- With regard to the examples of data breaches at other organisations, the fines levied by the Information Commissioner against organisation were still under previous Data Protection legislation; under GDPR these would have been higher.

- No meetings of the Information Governance Champions Group had been held, but meetings with individual members to progress and review their ongoing work.

- Work was ongoing across the University on Privacy Impact Assessment audits, Layered Privacy Notices and Data Sharing Agreements.

- Ten Subject Access Requests had been received, with one being reported to the Information Commissioner.

- Records Retention Schedules for Information Services and Equate Scotland were near completion. Work on the RRS for Human Resources was ongoing, and had been initiated for the Screen Academy.

07	Data Protection Ongoing Compliance Plan and Upcoming Internal Audit	Verbal Report

The Information Governance Manager reported on the current matters regarding Data Protection Compliance and Internal Audit.

The IGM requested feedback from members regarding areas of the University that could be assessed for the upcoming internal audit.

The University's information asset register required to be review, in order to be at a standard suitable to present to the Information Commissioner's Office.

A 'Right to be Forgotten' request had highlighted the need for governance processes to be reviewed. Some of the University's systems were not designed to suitably delete data.

A recent data breach had occurred when a spam filter malfunctioned and a large number of emails had been sent out to incorrect recipients. Information Services' response had caught the majority of the emails sent to internal recipients, but not some sent to externals. Members were requested to check with colleagues to discourage the use of email to transport sensitive data.

The IT Business Change Consultant noted that there are possibilities with existing and forthcoming Microsoft systems that could be used by the University to improve security. For instance SharePoint to Cloud had potential to lock down security settings, and Office365 could offer the opportunity to side-line file sharing services such as Dropbox.

The IGM stated that she planned to reconvene the Information Governance Champions Group, which would assist co-ordination and awareness of the work being done across the University.

08	Student Privacy Notice (For Discussion)	Verbal Report

The Information Governance Manager reported on the current matters regarding Student Privacy Notices.

Rather than the previous 'one size fits all' approach, it was being considered that individual areas or schools could have privacy notices tailored to their specific requirements. Additionally, privacy notices required more information on partnerships.

There were potential issues with students studying abroad, particularly with organisations that would not sign up to data sharing agreements.

Contact with students via social media also presented potential issues. The Information Commissioner's Office was considering these. An internal project was exploring the potential to use Facebook Workplace, but there were possible issues with Facebook itself.

The IGM emphasised that care needed to be taken with the use of social media in the context of processing student personal data.

09	CCTV Code of Conduct (For Approval)	UIGG(18/19)05

The Information Governance Manager reported on the current version of the CCTV Code of Conduct, and noted that while CCTV had previously been the responsibility of Security, it was planned to move this under Property and Facilities. New forms were being devised, to reflect the change.

CCTV was considered a high-risk area; the University had approximately 500 cameras. A joint project with Security and Property and Facilities had begun in order to rationalise CCTV provision on the University's estate.

An update on CCTV would be brought to a future meeting of UIGG.

The CCTV Code of Conduct was **approved**.

10	Data Protection Policy Statement (For Review)	UIGG(18/19)06

The Information Governance Manager noted that the Data Protection Policy Statement had been updated to take account of GDPR. Members were requested to feed back any further changes that might be required.

The Data Protection Policy Statement was **approved**.

11	Information Services Update	Verbal Report

The IT Business Change Consultant reported on current Information Services matters:
- Uptake of the online training had been poor – at January 2019 only 311 of 2652 staff listed in HR Connect had completed the course, despite it being made mandatory and communicated to Heads of Service / Directors.
- A project had been initiated to implement MFA (Multi Factor Authentication) to strengthen the security of Office 365 accounts
- A project had been initiated to implement SIEM (Security Information and Event Management) to allow the security team to better detect attacks and data breaches
- Cyber Essentials + certification had been achieved

- An update on the follow on actions from the Staff to Office 365 email project (now closed) was given – establishing governance/naming conventions around Groups/Teams and a strategy for data categorisation across the Office 365 platform.
- Lessons learned from the Remote Access to Data project included ensuring we take the needs of all University "niche" groups into consideration when planning services – including some research funding councils insisting on data being held on University premises and the need for off-line access by staff working in areas where a persistent internet connection was not possible. The use of Cloud based services was being explored as the first option for sharing of data which brought with it both risks but also opportunities to further secure and track access to University data.
- The SharePoint to the Cloud project planned to migrate the newly reviewed and reorganised Information Services staff workplace team site to SharePoint in Office 365 in March as early adopters/beta testers.
- A project to implement Identity Management/review staff account creation process was also in progress.

Remaining meeting dates for 2018/19

Thursday 13 June 2019 (10.00 am – 12.00 noon), Glassroom, Merchiston Campus